УДК 004.415.53:621.791 https://doi.org/10.32515/2664-262X.2025.12(43).2.36-54

Т. В. Смірнова[1], канд. техн. наук, **К. О. Буравченко**[1], доц., канд. техн. наук,
О. А. Добринчук[2], мол. наук. співр., **С. А. Смірнов**[1], доц., канд. техн. наук,
Н. М. Якименко[1], доц., канд. фіз.-мат. наук, **О. А. Смірнов**[1], проф., д-р техн. наук
[1]*Центральноукраїнський національний технічний університет, Кропивницький, Україна*
[2]*Державний університет "Київський авіаційний інститут", Київ, Україна*
e-mail: sm.tetyana@gmail.com, buravchenkok@gmail.com, dobrynchuk85@icloud.com, smirnov.ser.81@gmail.com, kntukafpz@gmail.com, dr.smirnovoa@gmail.com

Хмарна технологія моніторингу ключових індикаторів ефективності технологічних процесів у критичній інфраструктурі

В роботі розроблена хмарна технологія для моніторингу ключових індикаторів ефективності технологічних процесів критичної інфраструктури у реальному часі з метою виявлення відхилень у технологічних процесах, а також для попередження атак (збоїв) шляхом аналізу аномальної поведінки обладнання, зміни режимів навантаження, споживання ресурсів тощо. Отримала подальший розвиток кортежна модель ключових індикаторів ефективності, яка дозволяє систематизувати параметри моніторингу в інформаційно-комунікаційних системах об'єктів критичної інфраструктури, формалізувати автоматичну обробку даних, підтримати інтеграцію з аналітичними хмарними платформами, а також визначити відхилення (аномалії), кіберінциденти, деградацію, надмірне навантаження або саботаж і, як наслідок, підготувати агрегованих ключових індикаторів ефективності для щоденного моніторингу операторами та IT-службами. Запропоновано модель технологічного процесу електродугової обробки в інженерії БПЛА, яка в умовах сучасного етапу російсько-української війни є частиною критичної інфраструктури у секторі економіки та оборонно-промислового виробництва. Це пов'язано з тим, що БПЛА відіграють зараз вирішальну роль на полі бою. Розроблено схему моніторингу ключових індикаторів ефективності для технологічного процесу електродугової обробки. Для цього запропоновано використання хмарних технологій, наведено загальну схему технологічного процесу електродугової обробки в інженерії БПЛА, з їх використанням. Реалізовано приклад інфраструктури моделі на основі хмарної платформи Azure. Модель даних представлена у форматі JSON (який є ефективним для API, MQTT-брокера або Kafka). Перевірка моделі на емпіричних даних підтвердила її відповідність вимогам, стійкість до зміни умов та велику значимість для моніторингу технологічних процесів у критичній інфраструктурі. В умовах цифровізації та протидії кіберризикам модель є основою для створення цифрового двійника виробничої системи. Таким чином забезпечується надійність, прогнозованість і безпека. У роботі запропонована інтеграція з алгоритмами штучного інтелекту/машинного навчання (AI/ML), такими як LSTM, що дозволяє у режимі реального часу розширену аналітику, адаптивне управління процесом та автоматизоване прийняття рішень. У перспективі зазначений алгоритм LSTM можна використати для побудови моделі прогнозування параметрів ключових індикаторів ефективності у системі електродугової обробки, також можна використати інші алгоритми AI/ML та інтелектуального аналізу даних, які здатні обробляти великі обсяги часових рядів та враховувати складні нелінійні залежності між технологічними параметрами.

хмарна технологія, технологічні процеси, критична інфраструктура, інформаційно-комунікаційна система, електродугова обробка, БПЛА, кіберризики, кібербезпека, інтернет речей, штучний інтелект, машинне навчання

Постановка проблеми. У сучасних умовах цифрової трансформації державного управління, промисловості та енергетики, критична інфраструктура (КІ) держави стає дедалі більш залежною від інформаційно-комунікаційних технологій (ІКТ) та їх сервісів [1]. Автоматизовані системи керування технологічними процесами (АСУ ТП), промислові IoT-рішення та цифрові платформи забезпечують безперервність, продуктивність і точність виробничих та інфраструктурних операцій. Проте зростання складності цих систем вимагає переходу від традиційного моніторингу до інтелектуального аналізу ключових індикаторів ефективності (KPI, Key Performance

Indicators), що відображають як технічний, так і економічний стан функціонування об'єктів КІ. Стрімке переведення інформації у цифрову форму приводить до зростання кількості та складності кіберзагроз, спрямованих саме на об'єкти КІ [2], до яких відносяться об'єкти енергетичної структури, транспортної мережі, водопостачання, зв'язку, закладів охорони здоров'я.

Атаки типу ransomware, складні APT-кампанії, виведення з ладу SCADA-компонентів і вторгнення у хмарні сервіси демонструють, що стандартні методи контролю більше не є достатніми. Умови повномасштабної війни показали, що транспортні вузли, засоби телекомунікації, енергетичні системи, об'єкти охорони здоров'я України перебувають під постійною загрозою. Країна агресор постійно атакує об'єкти КІ поєднуючи з цілеспрямованими кібератаками на автоматизовані системи управління. Тиск з усіх боків вимагає не лише фізичного захисту об'єктів, а й оперативного цифрового відстежування функціонального стану обладнання, що дозволяє швидко реагувати на нестандартні або шкідливі дії різного характеру. Відповідно до цього, система відстежування ключових показників ефективності, яка впроваджується з застосуванням хмарних технологій та елементів реалізації кіберзахисту, повинна стати, навіть в умовах бойових дій або перебоїв зв'язку з окремими об'єктами, ключовим засобом підтримки стійкості й відновлення інфраструктури в реальному часі.

Монторинг KPI дозволяє у реальному часі визначити відхилення у технологічних процесах. Крім того, цей моніторинг дозволяє попередити наслідки атак за рахунок аналізу нестандартної поведінки обладнання, аномальної зміни режимів навантаження та споживання ресурсів. Застосування хмарних технологій дозволяє реалізувати нові можливості відстежування показників ефективності (KPI) з віддаленим доступом і централізованим керування, що є більш масштабним, надійним та безпечним. Використання хмарних сервісів дозволяє об'єднання даних з географічно розподілених об'єктів, а застосування AI/ML дозволяє знаходити приховані загрози та передбачити збої обладнання під час реалізації технологічного процесу. Таким чином, використання хмарних технологій для відстежування KPI у сфері КІ, в умовах повномасштабного вторгнення, гібридної війни, ризиків техногенних катастроф та тероризму, є стратегічно значущим кроком у забезпеченні кіберстійкості держави, а не лише тільки потрібним технологічним рішенням [3].

Метою дослідження є виявлення відхилень у технологічних процесах, а також попередження атак (збоїв) шляхом аналізу аномальної поведінки обладнання, зміни режимів навантаження, споживання ресурсів тощо.

Аналіз останніх досліджень і публікацій. Проведений аналіз [4-7] показав, що індекси KPI вказують на параметри стану технологічних процесів, технічного обладнання, безпеки, економічної та організаційної продуктивності, які є критично важливими. Для спостереження за цими індексами необхідна висока швидкість обробки даних, забезпечення надійності та впровадження масштабованості. Врахування усього цього обґрунтовує використання хмарних платформ, як багатообіцяючої бази реалізації систем моніторингу індексів KPI.

Використання сучасних хмарних платформ, таких як AWS, Microsoft Azure, Google Cloud, IBM Cloud, надає можливість обробляти гетерогенні потоки даних з різних джерел даних, до яких можливо віднести IoT-сенсори, SCADA-системи, ERP/CRM-системи, логістичні модулі. Це дозволяє створювати потужні сервіси для побудови систем збору, обробки, зберігання та аналітики великих даних в режимі реального часу, у межах єдиної хмарної архітектури. Хмарна інфраструктура забезпечує гнучкий доступ до KPI, інструменти для їхньої візуалізації (через Grafana,

Power BI, Kibana), а також інтеграцію з модулями AI/ML, які дають змогу прогнозувати аномалії та ризики ще до настання критичних подій.

Останні наукові дослідження демонструють переваги хмарних рішень у критичних галузях, зокрема в енергетиці, транспорті, оборонній промисловості [4]. Доведено, що використання хмарних обчислень для KPI-аналітики підвищує швидкість реагування на відхилення в системах управління [5]. Перехід на PaaS-рішення з вбудованими KPI-модулями дозволяє значно знизити витрати на IT-інфраструктуру, про що засвідчують інші дослідження. Особливо перспективними вважаються хмарні сервіси з підтримкою Edge Computing, які дозволяють обробляти дані максимально близько до джерел (датчиків, контролерів) і синхронізувати їх із центральними дашбордами в хмарі [6, 7].

Водночас існують і виклики: ризики втрати конфіденційності даних, залежність від постачальників хмарних послуг (vendor lock-in), необхідність відповідності нормативам безпеки (GDPR, ISO/IEC 27017, NIST 800-53). У відповідь на це активно розвиваються моделі гібридних та приватних хмар, що дозволяють реалізувати критично важливі системи моніторингу в умовах підвищених вимог до безпеки й контролю над даними [8-10].

Таким чином можливо зробити висновок, що застосування хмарних технологій для моніторингу індексів ключових індикаторів ефективності (KPI) являє собою перспективний науковий та практичний напрямок. Такий підхід поєднує аналітику великих даних, моделі прогнозування, оперативну візуалізацію та централізоване управління у єдиному середовищі.

Постановка завдання. У даному дослідженні необхідно розробити хмарну технологію для моніторингу ключових індикаторів ефективності технологічних процесів критичної інфраструктури у реальному часі з метою виявлення відхилень у технологічних процесах, а також попередження атак (збоїв) шляхом аналізу аномальної поведінки обладнання, зміни режимів навантаження, споживання ресурсів тощо.

Виклад основного матеріалу. *Кортежна модель моніторингу ключових індикаторів ефективності технологічних процесів у критичній інфраструктурі*

Для розроблення узагальненої формалізованої кортежної моделі ключових індикаторів ефективності технологічних процесів у КІ, використовуючи теорію множин [11-13], необхідно визначити найбільш важливі індикатори ефективності (множини), виконавши наступні кроки:

Крок 1. Визначимо множину об'єктів моніторингу:

$$O = \{\bigcup_{i=1}^{n} O_i\} = \{O_1, O_2, \dots, O_n\}, \quad (1)$$

де $O_i \subseteq O$ $(i = \overline{1,n})$ – об'єкти моніторингу (сервер, насос, трансформатор, лінія зв'язку, SCADA-модуль, технологічна лінія тощо), з яких система братиме певні параметри для подальшого аналізу.

Крок 2. Визначимо множину параметрів процесу:

$$P = \left\{\bigcup_{i=1}^{k} P_i\right\} = \{P_1, P_2, \dots, P_k\}, \quad (2)$$

де $P_i \subseteq P$ $\left(i = \overline{1,k}\right)$ – один з контрольованих системою параметрів (фізичних, логічних, кіберпараметрів тощо), що вимірюється певним пристроєм за допомогою певного методу вимірювання (наприклад, температура, тиск, затримка, навантаження, напруга живлення тощо).

Крок Визначимо множину методів вимірювання:

$$M = P \to \mathcal{F}, \quad (3)$$

де $\mathcal{F} = \{\text{сенсори, логфайли, метрики з API, агетнські дані}\}$, що є фактичним відображенням параметрів P_i у методи збору даних.

Крок 4. Визначимо множину інтервалів спостереження:

$$T = \{\bigcup_{i=1}^{m} T_i\} = \{T_1, T_2, \dots, T_m\}, \quad (4)$$

де $T_i \in \mathbb{R}$ – конкретний часовий інтервал або дискрет, протягом якого здійснюється вимірювання $\mathcal{F}$ певних параметрів процесу P_i .

Крок 5. Визначимо множину допустимих або нормативних значень KPI:

$$D = \left\{\bigcup_{i=1}^{k} D_i\right\} = \{D_1, D_2, \dots, D_k\}, \quad (5)$$

де $D_i = [minP_i; maxP_i]$ – допустимі або нормативні значення параметрів P_i KPI.

Крок 6. Визначимо множину значень KPI у певний момент часу:

$$V = \left\{\bigcup_{i=1}^{k} V_i\right\} = \{V_1, V_2, \dots, V_k\}, \quad (6)$$

де $V_i = \{v_{i,t} \in \mathbb{R} | P_i \subseteq P, t \in T\}$ – реальні виміряні значення параметрів P_i KPI в момент часу t.

Крок 7. Визначимо множину правил обробки та агрегації даних (KPI):

$$R = \{f_1, f_2, \dots, f_l\}, \quad (7)$$

де $f_i \subseteq f\ (i = \overline{1,l}\ ),\ \ f_i : V \to \mathbb{R}$ – функціонали, що описують правила аналізу KPI (для прикладу, усереднення, максимум / мінімум, похідна, тренд тощо).

Крок 8. Визначимо множину способів семантичної інтерпретації отриманих станів KPI:

$$A = \left\{\bigcup_{i=1}^{p} A_i\right\} = \left\{A_1, A_2, \dots, A_p\right\}, \quad (8)$$

де $A_i \subseteq A\ (i = \overline{1,p}\ )$ – спосіб семантичної інтерпретації стану KPI (наприклад, «нормальний», «аномальний», «загроза», «критичний стан», «помилка», «аварія», «кризова ситуація» тощо).

Відповідно, функцію виявлення аномалії можна представити наступним чином:

$$\delta: V \times D \to A. \quad (9)$$

З урахуванням (1) – (8) формалізована кортежна модель KPI технологічних процесів у КІ можна представити у вигляді кортежу параметрів:

$$\text{KPI} = \left\{\bigcup_{i=1}^{q} KPI_i\right\} = \left\{KPI_1, KPI_2, \dots, KPI_q\right\}, \quad (10)$$

де $KPI_i \subseteq KPI\ (i = \overline{1,q}\ )$ – ключові індикатори ефективності технологічних процесів у КІ.

Отримана кортежна модель KPI (10) дозволяє систематизувати параметри моніторингу в ІКС об'єктів КІ, формалізувати автоматичну обробку даних, підтримати інтеграцію з аналітичними хмарними платформами (Prometheus, Azure Monitor, Grafana, etc.), а також визначити відхилення (аномалії), кіберінциденти, деградацію, надмірне навантаження або саботаж і, як наслідок, підготувати агреговані KPI для щоденного моніторингу операторами та ІТ-службами.

На рисунку 1 представлене схематичне відображення моделі, яка є узагальненим відображенням процесу моніторингу ключових показників ефективності будь-яких технологічних процесів, що реалізуються в секторах КІ держави [14-15].

У наступному підпункті даної роботи буде розглянуто приклад реалізації зазначеної моделі для технологічного процесу електродугової обробки (ЕДО) [16-18] в інженерії БПЛА.

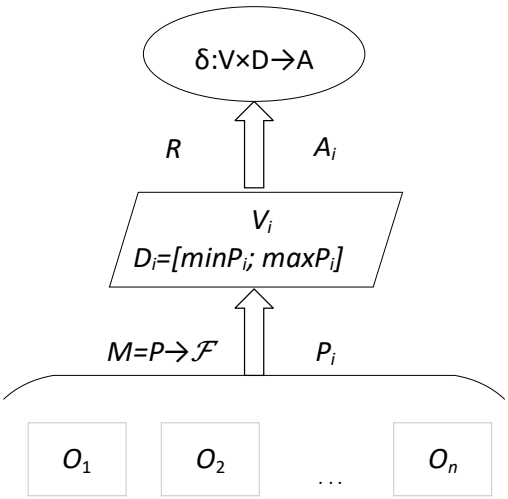

Рисунок 1 – Схематичне відображення моделі моніторингу ключових індикаторів ефективності технологічних процесів

Джерело: розроблено авторами

Приклад практичної реалізації кортежної моделі моніторингу ключових індикаторів ефективності технологічного процесу ЕДО в інженерії БПЛА

ЕДО є одним із ключових технологічних процесів в авіаційній інженерії, який забезпечує високоточне виготовлення, модифікацію або відновлення критичних деталей літальних апаратів. Завдяки використанню дугового розряду, що виникає між електродом і оброблюваною поверхнею, досягається локалізоване плавлення матеріалу з мінімальним тепловим впливом на прилеглі зони. Це особливо важливо при роботі з високолегованими, тугоплавкими або термочутливими сплавами, які широко застосовуються в авіаційних конструкціях – зокрема, в елементах двигунів, шасі, паливних системах, та каркасних компонентах літаків і БПЛА.

У виробництві та ремонті авіаційної техніки ЕДО використовується як для формування нових деталей методом наплавлення або дугового різання, так і для відновлення зношених поверхонь. Наприклад, нанесення зносостійкого шару на крайку лопатки компресора турбореактивного двигуна дозволяє значно подовжити її експлуатаційний ресурс без необхідності повної заміни. Крім того, електродугова наплавка використовується для ремонту тріщин, пор або зношених отворів у корпусних елементах, де точність і надійність шва мають критичне значення. Завдяки можливості точного контролю струму, напруги, швидкості подачі електрода і траєкторії наплавлення, ЕДО забезпечує необхідні механічні властивості з'єднання – міцність, герметичність, ударостійкість – без ризику структурної деформації або перегріву.

Ще одним важливим аспектом застосування ЕДО в авіації є можливість її інтеграції з автоматизованими та роботизованими системами, що підвищує відтворюваність, продуктивність та безпеку процесу. При великосерійному виробництві та обробці деталей складної геометрії, а саме таким є виробництво БПЛА, що набрало надзвичайну актуальність на сучасному етапі повномасштабного вторгнення, людський фактор може стати причиною помилки або помилок, тому ця інтеграція є надзвичайно необхідною. Застосування новітніх наукових розробок дозволяє об’єднувати системи ЕДО з сучасними технологіями машинного зору, цифрового моніторингу KPI та контролю якості у режимі реального часу. Це робить їх у рамках авіаційної промисловості невід'ємним складником концепції «розумного виробництва» (Smart Manufacturing) [19-20]. Тому, можемо зробити висновок щодо ЕДО, як провідної технології, що дозволяє в умовах жорстких нормативних вимог до

авіаційної техніки, забезпечити високу надійність та точність виробництва, яка потрібна при виробництві БПЛА.

У сфері БПЛА технологія ЕДО набуває дедалі більшого значення як ефективна технологія для виготовлення, ремонту та модернізації компонентів, що зазнають значних механічних і термічних навантажень. Зокрема, ЕДО активно використовується для наплавлення зносостійких або антикорозійних шарів на деталі, що входять до складу силової установки, елементів шасі або вузлів кріплення крил. В умовах, коли БПЛА часто експлуатуються в агресивному середовищі – пил, волога, температурні коливання, – такі технології дозволяють не тільки підвищити ресурс техніки, а й адаптувати її до специфічних умов бойового чи цивільного застосування.

Особливої актуальності ЕДО набуває при виробництві тактичних БПЛА, які мають невеликі розміри, але потребують високої точності виготовлення та структурної міцності. При такому виробництві ЕДО використовується для формування несучих елементів каркасу, кріплень гвинтових агрегатів, деталей систем посадки. Це реалізується даним технологічним процесом завдячуючи локальній дії та можливості роботи з композиційними матеріалами або сплавами на основі титану й алюмінію. Також технологія активно впроваджується для створення захисних екранів і демпферів у БПЛА, що несуть на борту електроніку, оптичні прилади чи корисне навантаження – дозволяючи формувати складні конструкції із вбудованим захистом за однопрохідний або багатопрохідний цикл обробки.

Крім виготовлення, ЕДО демонструє високу ефективність у відновлювальних процесах для БПЛА, що особливо важливо в умовах воєнного часу. Наприклад, пошкоджені під час бойових вильотів корпусні деталі або монтажні вузли можуть бути відремонтовані методами дугового наплавлення чи зварювання без повного демонтажу чи заміни. Це значно скорочує час відновлення й дає змогу оперативно повертати дрони до експлуатації. У перспективі поєднання ЕДО з адитивними технологіями (WAAM – Wire Arc Additive Manufacturing) [21] відкриває можливості для створення складних деталей БПЛА «з нуля» – без використання дорогих прес-форм або лиття, що критично важливо для розгортання польових ремонтно-виробничих модулів у зоні бойових дій. Таким чином, ЕДО виступає ключовим елементом інноваційного циклу життєвого забезпечення безпілотних систем.

Розглянемо частковий випадок реалізації моделі, розробленої вище для технологічного процесу ЕДО в інженерії БПЛА, враховуючи (1) – (9):

Крок 1. Визначимо множину об'єктів моніторингу при виготовленні БПЛА:

При n=3 (тобто в технологічному процесі ЕДО при виготовленні БПЛА в цеху використовується паралельно 3 установки, що забезпечують технологічний процес) вираз (1) матиме вигляд:

$$O = \{\bigcup_{i=1}^{3} O_i\} = \{O_1, O_2, O_3\} = \{EDO_1, EDO_2, EDO_3\},$$

де EDO_1, EDO_2, EDO_3 – це установки, що забезпечують технологічний процес ЕДО в цеху при виготовленні БПЛА.

Крок 2. Визначимо множину параметрів процесу ЕДО:

При k=5 (тобто в технологічному процесі ЕДО при виготовленні БПЛА в цеху важливими для моніторингу є 5 параметрів технологічного процесу) вираз (2) матиме вигляд:

$$P = \left\{\bigcup_{i=1}^{5} P_i\right\} = \{P_1, P_2, \dots, P_5\} = \{U, I, T, v, f\}, \quad (12)$$

де $P_1 = U$ – напруга, $P_2 = I$ – струм, $P_3 = T$ – температура зони обробки, $P_4 = v$ – швидкість подачі електрода, $P_5 = f$ – частота коливань дуги.

Крок Визначимо множину методів вимірювання параметрів процесу ЕДО:

При вимірюванні напруги, струму, температури зони обробки, швидкості подачі електрода та частоти коливань дуги вираз (3) з урахуванням (12) матиме такий вигляд:

$$M_1 = U, I \to \mathcal{F}_1,$$
$$M_2 = T \to \mathcal{F}_2,$$
$$M_3 = v \to \mathcal{F}_3,$$
$$M_4 = f \to \mathcal{F}_4,$$

де $\mathcal{F}_1$ – цифрові осцилографи через OPC/Modbus для вимірювання напруги і струму, $\mathcal{F}_2$ – термопари типу K із передачею по MQTT для вимірювання температури зони обробки, $\mathcal{F}_3$ – енкодери рухомих вузлів для вимірювання швидкості подачі електрода, $\mathcal{F}_4$ – аналіз сигналу від плазмотрону (Fourier/FFT) → Edge AI для вимірювання частоти коливань дуги.

Передавання даних відбувається через IoT-шлюзи до хмари (Azure IoT Hub / AWS Greengrass → AWS IoT Core).

Крок 4. Визначимо множину інтервалів спостереження, протягом яких здійснюється вимірювання в процесі ЕДО:

При m=3 (обрано три базові інтервали спостереження) вираз (4) матиме наступний вигляд:

$$T = \{\bigcup_{i=1}^{3} T_i\} = \{T_1, T_2, T_3\} = \{1, 5, 60\},$$

де $T_1 = 1$ с., $T_2 = 5$ с. та $T_3 = 60$ с. (агрегація) – це базові інтервали, протягом якого здійснюється вимірювання параметрів процесу ЕДО.

Крок 5. Визначимо множину допустимих або нормативних значень KPI процесу ЕДО:

При k=5 (як зазначалось, в технологічному процесі ЕДО при виготовленні БПЛА в цеху важливими для моніторингу є 5 параметрів технологічного процесу, відповідно кожен параметр має певні граничні значення) вираз (5) матиме вигляд:

$$D = \left\{\bigcup_{i=1}^{5} D_i\right\} = \{D_1, D_2, \dots, D_5\} = \{[minP_1; maxP_1], [minP_2; maxP_2],$$
$$[minP_3; maxP_3], [minP_4; maxP_4], [minP_5; maxP_5]\} = \{[80; 120], [100; 180],$$
$$[900; 1300], [0{,}2; 1{,}0], [1000; 1300]\},$$

де $D_1 = [minP_1; maxP_1] = [80; 120]$ – граничні значення напруги (у Вольтах, В), $D_2 = [minP_2; maxP_2] = [100; 180]$ – граничні значення сили струму (в Амперах, А), $D_3 = [minP_3; maxP_3] = [900; 1300]$ – граничні значення температури зони обробки (у градусах Цельсія, °С), $D_4 = [minP_4; maxP_4] = [0{,}2; 1{,}0]$ – граничні значення швидкості подачі електрода (у сантиметрах на секунду, см/с), $D_5 = [minP_5; maxP_5] = [1000; 1300]$ – граничні значення частоти коливань дуги (у Герцах, Гц).

Крок 6. Визначимо множину значень KPI, виміряних у певний момент часу в процесі ЕДО:

При k=5 (як зазначалось, в технологічному процесі ЕДО при виготовленні БПЛА в цеху важливими для моніторингу є 5 параметрів технологічного процесу) вираз (6) матиме вигляд:

$$V = \left\{\bigcup_{i=1}^{5} V_i\right\} = \{V_1, V_2, \dots, V_5\} = \{100, 150, 1400, 1, 1100\},,$$

де $V_1 = 100, V_2 = 150, V_3 = 1400, V_4 = 1, V_5 = 1100$ – реальні виміряні значення параметрів KPI (напруга, струм, температура зони обробки, швидкість подачі електрода та частота коливань дуги відповідно) в момент часу t.

Отримані дані передаються у хмарну СУБД (наприклад, AWS Timestream або Azure Data Explorer) або в InfluxDB для часових рядів та подальшого їх аналізу системою.

Крок 7. Визначимо множину правил обробки та агрегації даних, отриманих від системи моніторингу в процесі ЕДО:

При l=5 вираз (7) матиме наступний вигляд:

$R = \{f_1, f_2, \dots, f_l\} = \{f_1, f_2, \dots, f_5\} = \{f_{trend}(U),\ f_{mean}(I), f_{std}(T)\ , f_{mean}(v), f_{FFT}(f)\}$,
де $f_1 = f_{trend}(U)$ – лінійна регресія зміни напруги, $f_2 = f_{mean}(I)$ – середній струм за хвилину (наприклад 150 А), $f_3 = f_{std}(T)$ – відхилення температури (наприклад, 100°С), $f_4 = f_{mean}(v)$ – середня швидкість подачі електрода (для прикладу, 0,5 см/с), $f_5 = f_{FFT}(f)$ – гармонійний аналіз коливань дуги.

Обробка даних здійснюється через хмарні платформи AWS Lambda / Azure Functions або Spark Streaming.

Крок 8. Визначимо множину способів семантичної інтерпретації отриманих станів KPI системи моніторингу в процесі ЕДО:

При p=9 вираз (8) матиме наступний вигляд:

$$A = \{\bigcup_{i=1}^{9} A_i\} = \{A_1, A_2, \dots, A_9\} = \{NORMAL,\ ANOMALY,\ THREAT,\ CRITICAL,\ ERROR,\ CRISIS,\ DISASTER,\ WARNING,\ DEVIATION\},$$

де $A_1 = NORMAL,\ A_2 = ANOMALY,\ A_3 = THREAT,\ A_4 = CRITICAL,\ A_5 = ERROR,\ A_6 = CRISIS,\ A_7 = DISASTER,\ A_8 = WARNING, A_9 = DEVIATION$ – визначені способи семантичної інтерпретації стану KPI на основі аналізу параметрів (аномалія, загроза, критично, помилка, криза, аварійний стан, увага, відхилення відповідно).

Функцію виявлення аномалії можна реалізувати, наприклад, через Threshold Alerts (Prometheus, Azure Monitor) чи AI-based detection (наприклад, anomaly detection в Azure Synapse ML або Amazon Lookout for Metrics). Тоді, враховуючи (9), вона матиме наступний вигляд:

$$\delta: V \times D \to A \in \{NORMAL, NORMAL, DEVIATION, NORMAL, NORMAL,\}$$

Враховуючи виконані кроки згідно (1) – (8) частковий випадок кортежної моделі (10) для технологічного процесу ЕДО в інженерії БПЛА (при $q = 8$) матиме такий вигляд:

$$\text{KPI}_{EDO} = \{\bigcup_{i=1}^{8} KPI_i\} = \{KPI_1, KPI_2, \dots, KPI_8\} = \{O, P, M, T, D, V, R, A\}. \quad (13)$$

Відповідно, схематично розроблену модель моніторингу ключових індикаторів ефективності технологічних процесів, що розроблена в попередньому підрозділі і представлена на рисунку 1 для технологічного процесу ЕДО в інженерії БПЛА можна представити наступним чином:

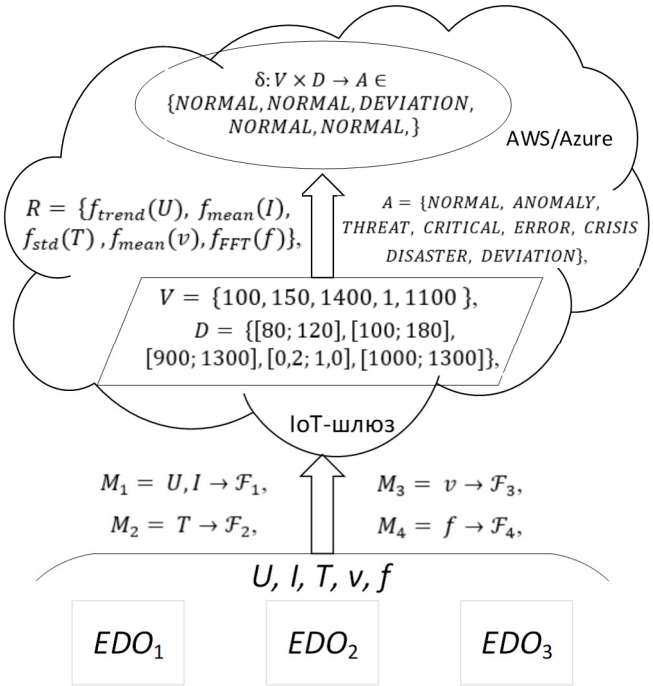

Рисунок 2 – Схематичне відображення моделі моніторингу ключових індикаторів ефективності для технологічного процесу ЕДО

Джерело: розроблено авторами

Приклад інфраструктури реалізації моделі в хмарі Azure (обраний сервіс не є обов'язковим для застосування, а використовується лише як наглядний приклад – може бути використано будь-який інший рівноцінний за функціоналом сервіс) наведено на рисунку 3:

```
[Sensor → Edge Gateway]
        ↓ MQTT/OPC-UA
  Azure IoT Hub
        ↓
  Stream Analytics → Azure Data Lake / Cosmos DB
        ↓
  Azure ML Studio (Anomaly Detection)
        ↓
  Power BI / Grafana
```

Рисунок 3 – Варіант інфраструктури реалізації моделі в хмарі

Джерело: розроблено авторами

Модель даних у форматі JSON, що є зручним представленням для API, MQTT-брокера або Kafka, відображено на рисунку 4:

```
{
  "KPI": {
    "object": "EDO_Station_01",
    "parameters": {
      "current": { "value": 175, "unit": "A", "status": "OK" },
      "temperature": { "value": 1200, "unit": "C", "status": "Warning" }
    },
    "timestamp": "2025-07-18T10:05:00Z"
  }
}
```

Рисунок 4 – JSON модель даних

Джерело: розроблено авторами

Схема технологічного процесу ЕДО в інженерії БПЛА на основі хмарних технологій, для якого представлено частковий випадок кортежної моделі (13), відображена на рисунку 5:

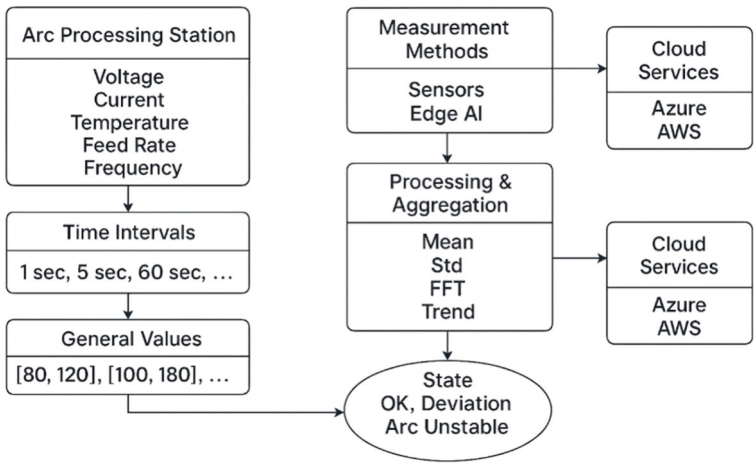

Рисунок 5 – Схема технологічного процесу ЕДО в інженерії БПЛА на основі хмарних технологій

Джерело: розроблено авторами

Наступний підрозділ даної роботи присвячений верифікації розробленої моделі у контексті її придатності до практичної імплементації.

4. Верифікація моделі моніторингу ключових індикаторів ефективності технологічного процесу ЕДО в інженерії БПЛА

Згідно [12] визначено множину параметрів $P = \{U, I, T, v, f\}$, яка є важливою для технологічного процесу ЕДО в інженерії БПЛА. Одним із ключових параметрів є струм I. Верифікуємо модель на прикладі зазначеного параметру. Як зазначалось в п. 3 граничними значеннями сили струму, вимірюваної в амперах, є $[100; 180]$. Дослідимо вплив зміни параметру струму на KPI на інтервалі спостереження $T_3 = 60$ с. На рис. 6 відображено яким чином значення I впливає на кінцеву функцію виявлення аномалії $\delta: V \times D \to A$.

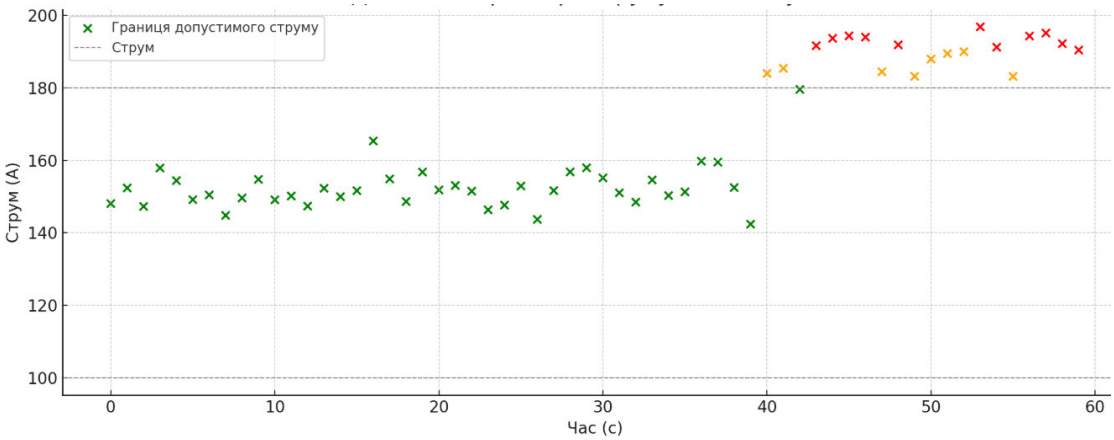

Рисунок 6 – Вплив відхилення сили струму I на статус KPI

Джерело: розроблено авторами

На рисунку 6 можна побачити, як струм змінюється протягом часу, а також визначено його KPI-статус згідно (8) – (9) на основі встановлених у моделі обмежень (граничних значень). У другій частині симуляції моделюється відхилення (перевищення), що призводить до появи негативних статусів, що демонструє роботу кортежної моделі у динаміці (табл. 1).

Таблиця 1 – Результати моделювання струму I протягом інтервалу T_3

***Час*, с**	***I*, А**	**А (статус KPI)**
0	148.05	NORMAL
1	152.35	NORMAL
2	147.25	NORMAL
3	157.86	NORMAL
4	154.39	NORMAL
5	149.13	NORMAL
6	150.42	NORMAL
7	144.78	NORMAL
8	149.58	NORMAL
9	154.72	NORMAL
10	149.08	NORMAL
11	150.13	NORMAL
12	147.34	NORMAL
13	152.25	NORMAL
14	149.94	NORMAL
15	151.61	NORMAL

Продовження таблиці 1

16	165.32	NORMAL
17	154.84	NORMAL
18	148.61	NORMAL
19	156.74	NORMAL
20	151.8	NORMAL
21	1504	NORMAL
22	151.47	NORMAL
23	146.32	NORMAL
24	147.61	NORMAL
25	152.89	NORMAL
26	1467	NORMAL
27	151.62	NORMAL
28	156.79	NORMAL
29	157.91	NORMAL
30	155.14	NORMAL
31	151.01	NORMAL
32	148.45	NORMAL
33	154.57	NORMAL
34	150.26	NORMAL
35	151.27	NORMAL
36	159.73	NORMAL
37	159.48	NORMAL
39	152.47	NORMAL
40	142.37	NORMAL
41	1895	WARNING
42	185.37	WARNING
43	179.55	NORMAL
44	191.61	CRITICAL
45	1966	CRITICAL
46	194.33	CRITICAL
47	1998	CRITICAL
48	184.43	WARNING
49	191.85	CRITICAL
50	1817	WARNING
51	187.94	WARNING
52	189.44	WARNING
53	189.97	WARNING
54	196.82	CRITICAL
55	191.2	CRITICAL
56	1814	WARNING
57	194.28	CRITICAL
58	195.11	CRITICAL
59	192.18	CRITICAL

Джерело: розроблено авторами

З рис. 6 та таблиці 1 наглядно видно, що починаючи з 41-ї секунди значення струму *I* знижується і з'являються негативні статуси KPI, які передаються системою моніторингу до центру прийняття рішень.

Підвищення струму понад 180 А у системі ЕДО викликає ланцюгову реакцію ризиків – від деградації обладнання до зниження якості виробу, що є особливо небезпечним у контексті виготовлення відповідальних компонентів для авіації або

БПЛА. Саме тому в кортежній моделі KPI перевищення струму призводить до статусу CRITICAL, що має ініціювати негайне реагування системи моніторингу.

Для порівняння розглянемо інші два важливі для технологічного процесу ЕДО в інженерії БПЛА параметри з кортежу $P = \{U, I, T, v, f\}$ – це напруга U (рисунок 7) та температура T (рисунок 8).

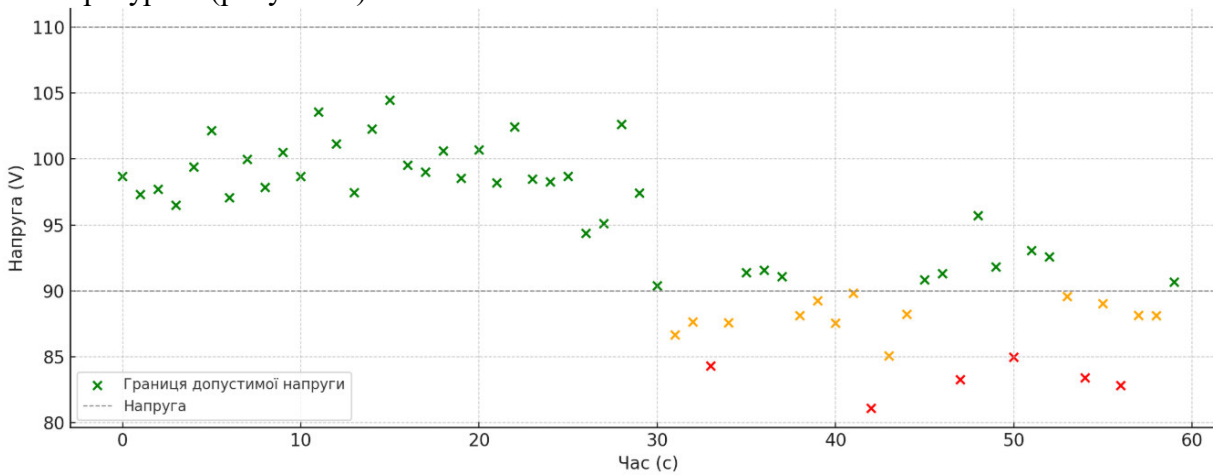

Рисунок 7 – Вплив відхилення напруги U на статус KPI

Джерело: розроблено авторами

Рисунок 7 ілюструє зміну напруги U в технологічному процесі, де видно, як вона спочатку знаходиться в межах норми, а після 30-ї секунди знижується нижче допустимого рівня, що викликає негативні статуси KPI, що демонструє роботу кортежної моделі у динаміці (табл. 2).

Таблиця 2 – Результати моделювання напруги U протягом інтервалу T_3

***Час*, с**	***U*, В**	**A (статус KPI)**
0	98.67	NORMAL
1	97.3	NORMAL
2	97.7	NORMAL
3	96.49	NORMAL
4	99.39	NORMAL
5	102.15	NORMAL
6	97.06	NORMAL
7	99.97	NORMAL
8	97.84	NORMAL
9	100.5	NORMAL
10	98.67	NORMAL
11	1056	NORMAL
12	101.14	NORMAL
13	97.44	NORMAL
14	102.27	NORMAL
15	104.46	NORMAL
16	99.52	NORMAL
17	99.0	NORMAL
18	100.61	NORMAL
19	98.53	NORMAL
20	100.69	NORMAL
21	98.19	NORMAL
22	102.43	NORMAL
23	98.47	NORMAL

Продовження таблиці 2

24	98.26	NORMAL
25	98.68	NORMAL
26	94.36	NORMAL
27	95.09	NORMAL
28	102.62	NORMAL
29	97.41	NORMAL
30	90.38	NORMAL
31	86.65	WARNING
32	87.63	WARNING
33	84.29	CRITICAL
34	87.57	WARNING
35	91.37	NORMAL
36	91.56	NORMAL
37	91.07	NORMAL
39	88.11	WARNING
40	89.24	WARNING
41	87.54	WARNING
42	89.81	WARNING
43	81.08	CRITICAL
44	85.06	WARNING
45	88.21	WARNING
46	90.83	NORMAL
47	91.3	NORMAL
48	825	CRITICAL
49	95.7	NORMAL
50	91.81	NORMAL
51	84.96	CRITICAL
52	905	NORMAL
53	92.57	NORMAL
54	89.56	WARNING
55	839	CRITICAL
56	89.02	WARNING
57	82.81	CRITICAL
58	88.13	WARNING
59	88.11	WARNING

Джерело: розроблено авторами

З рисунку 7 та таблиці 2 наглядно видно, що починаючи з 31-ї секунди значення напруги U знижується і з'являються негативні статуси KPI, які передаються системою моніторингу до центру прийняття рішень.

Зниження напруги нижче 90 В у системі ЕДО дестабілізує процес, погіршує якість обробки та створює приховану загрозу для обладнання. У критичних галузях – таких як авіація, БПЛА або оборонна промисловість – це може стати причиною виробничого браку або відмови в експлуатації. У системі моніторингу KPI така ситуація має класифікуватися як WARNING або CRITICAL, а також автоматично фіксуватися в хмарній аналітичній базі для подальшого аудиту.

Графік зміни температури T в технологічному процесі ЕДО та її KPI-статус у динаміці відображено на рисунку 8 (базується на моделювання – табл. 3). Як видно, після 30-ї секунди відбувається перевищення температури T вище допустимого порогу (1300 °C), що викликає негативні статуси KPI.

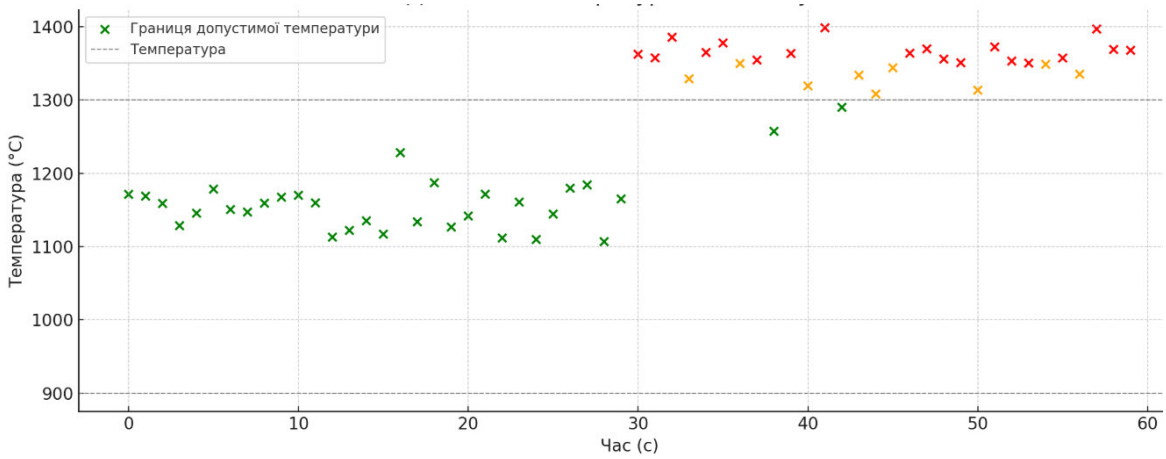

Рисунок 8 – Вплив відхилення температури T на статус KPI

Джерело: розроблено авторами

Таблиця 3 – Результати моделювання температури T протягом інтервалу T_3

***Час*, с**	***T*, °C**	**A (статус KPI)**
0	1171.22	NORMAL
1	1168.77	NORMAL
2	1158.77	NORMAL
3	1128.45	NORMAL
4	1145.48	NORMAL
5	1178.32	NORMAL
6	1150.48	NORMAL
7	1147.06	NORMAL
8	1159.14	NORMAL
9	1167.36	NORMAL
10	1169.91	NORMAL
11	1159.53	NORMAL
12	1112.83	NORMAL
13	1122.01	NORMAL
14	1135.1	NORMAL
15	1116.91	NORMAL
16	1228.09	NORMAL
17	11372	NORMAL
18	1187.02	NORMAL
19	1126.58	NORMAL
20	1141.67	NORMAL
21	1171.37	NORMAL
22	1111.68	NORMAL
23	1160.66	NORMAL
24	1109.59	NORMAL
25	1144.29	NORMAL
26	1179.61	NORMAL
27	1184.12	NORMAL
28	1106.71	NORMAL
29	1164.98	NORMAL
30	1362.36	CRITICAL
31	1357.43	CRITICAL
32	1385.59	CRITICAL
33	1328.85	WARNING

Продовження таблиці 3

34	1364.81	CRITICAL
35	1377.76	CRITICAL
36	1349.74	WARNING
37	1354.46	CRITICAL
39	1257.27	NORMAL
40	13642	CRITICAL
41	1319.15	WARNING
42	1398.48	CRITICAL
43	1289.99	NORMAL
44	13382	WARNING
45	1308.1	WARNING
46	13487	WARNING
47	13677	CRITICAL
48	1369.7	CRITICAL
49	1355.78	CRITICAL
50	1350.8	CRITICAL
51	13136	WARNING
52	1372.39	CRITICAL
53	13509	CRITICAL
54	1350.33	CRITICAL
55	1348.7	WARNING
56	1357.23	CRITICAL
57	1335.18	WARNING
58	1396.78	CRITICAL
59	1368.91	CRITICAL

Джерело: розроблено авторами

З рисунку 8 та таблиці 3 наглядно видно, що починаючи з 30-ї секунди значення температури T знижується і з'являються негативні статуси KPI, які передаються системою моніторингу до центру прийняття рішень.

Перевищення температури понад 1300 °C в ЕДО-системі є критичним порушенням, що несе загрозу як оброблюваним матеріалам, так і обладнанню. У моделі моніторингу ключових індикаторів ефективності таке відхилення має бути негайно ідентифіковано як CRITICAL, з подальшим автоматичним реагуванням – зупинка процесу, інформування персоналу, створення запису в системі хмарної аналітики та перегляд режимів обробки.

Існуючі методи AI/ML та інтелектуального аналізу даних застосовуються для обробки великих обсягів часових рядів та складних нелінійних залежностей між технологічними параметрами ЕДО. Саме ці методи доцільно застосовувати при побудові моделі прогнозування параметрів KPI у системі ЕДО. Застосування рекурентних нейронних мереж, а конкретно моделі довготривалої короткочасної пам'яті (LSTM), яка спеціалізується на аналізі послідовностей і здатна зберігати інформацію про попередні стани, що є важливим для технологічних процесів з інерційною динамікою, є одним з найефективніших підходів. Прогнозування майбутніх теплових та електричних значень, знаходження імовірно критичних тенденцій відхилення від нормативів, утворення сигналів попередження про настання аварійного або нештатного режиму, можливо якраз з високою точністю за рахунок використання моделі LSTM. Ця модель стає основою для побудови адаптивної системи моніторингу та управління KPI в ЕДО, у поєднанні з методами попередньої обробки даних (нормалізація, фільтрація шуму), використанням сенсорних IoT-даних та з хмарною

обчислювальною платформою. Це дозволяє підвищити безпеку та надійність процесів у критичній інфраструктурі, покращити якість обробки та знизити витрати на технічне обслуговування.

Висновки. Запропонована у даній роботі хмарна технологія моніторингу KPI технологічних процесів КІ, дозволяє у режимі реального часу виявляти відхилення у технологічних процесах, а також попереджувати атаки (кіберінциденти, збої). Це реалізовано за рахунок аналізу аномальної поведінки обладнання, зміни режимів навантаження, споживання ресурсів. У цьому контексті хмарні технології відкривають нові можливості для масштабованого, надійного і безпечного моніторингу показників ефективності з віддаленим доступом і централізованим керуванням.

Отримала подальший розвиток кортежна модель KPI, яка за рахунок визначення множин об'єктів моніторингу, параметрів процесу, методів вимірювання, інтервалів спостереження, допустимих (нормативних) значень KPI, значень KPI у певний момент часу, правил обробки та агрегації даних, способів семантичної інтерпретації отриманих станів KPI, а також застосування функції виявлення аномалії, дозволяє систематизувати параметри моніторингу в ІКС об'єктів КІ, формалізувати автоматичну обробку даних, підтримати інтеграцію з аналітичними хмарними платформами, а також визначити відхилення (аномалії), кіберінциденти, деградацію, надмірне навантаження або саботаж і, як наслідок, підготувати агреговані KPI для щоденного моніторингу операторами та IT-службами.

Розглянуто приклад реалізації розробленої моделі для технологічного процесу ЕДО в інженерії БПЛА, що є частиною КІ у секторі промисловості та оборонно-промислового виробництва, особливо коли йдеться про застосування в авіації, БПЛА або стратегічному машинобудуванні (це визначає підвищені вимоги до безпеки, надійності, контролю KPI та кіберзахисту таких систем). Також, розроблено схему моніторингу KPI для технологічного процесу ЕДО; наведено приклад інфраструктури реалізації моделі в хмарі Azure та модель даних у форматі JSON (що є зручним представленням для API, MQTT-брокера або Kafka), а також загальну схему технологічного процесу ЕДО в інженерії БПЛА на основі хмарних технологій.

Верифікація моделі на основі даних струму A, напруги U та температури T довела її функціональну коректність, стійкість до зміни умов і високу прикладну цінність для моніторингу технологічних процесів у КІ. Модель може стати основою для розробки цифрового двійника виробничої системи, забезпечуючи надійність, передбачуваність і безпеку в умовах цифровізації та кіберризиків, інтеграція з алгоритмами AI/ML, такими як LSTM, відкриває перспективу для розширеної аналітики, адаптивного управління процесом та автоматичного прийняття рішень у режимі реального часу. У перспективі зазначений алгоритм LSTM можна використати для побудови моделі прогнозування параметрів KPI у системі ЕДО, також можна використати інші алгоритми AI/ML та інтелектуального аналізу даних, які здатні обробляти великі обсяги часових рядів та враховувати складні нелінійні залежності між технологічними параметрами.

Список літератури

1. Gnatyuk S., Yudin O., Sydorenko V., Smirnova T., Polozhentsev A. The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems. *CEUR Workshop Proceedings.* 2022. Vol. 3156. P. 390–399.
2. Постанова КМУ «Деякі питання об'єктів критичної інфраструктури» від 9 жовтня 2020 р. № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#n11
3. Gnatyuk S., Berdibayev R., Smirnova T., Avkurova Z., Iavich M. Cloud-Based Cyber Incidents Response System and Software Tools. *Communications in Computer and Information Science.* 2021. Vol. 1486. P. 169–184.

4. Ardebili A. A., Martella C., Lazari A. et al. Smart Critical Infrastructures Security Management and Governance: Implementation of Cyber Resilience KPIs for Decentralized Energy Asset. *CEUR Workshop Proceedings.* 2024. Vol. 3731. URL: https://iris.unisalento.it/handle/11587/530328
5. Bridging measurement divides in AI, cloud, and cyber. URL: https://www.deloitte.com/us/en/insights/industry/technology/measuring-cyber-ai-and-cloud-kpis.html
6. Yıldırım F., Yalman Y., Bayındır K. Ç., Terciyanlı E. Comprehensive Review of Edge Computing for Power Systems: State of the Art, Architecture, and Applications. *Applied Sciences.* 2025. 15(8). 4592. https://doi.org/10.3390/app15084592
7. Wei X. et al. MVR: An Architecture for Computation Offloading in Mobile Edge Computing. *2017 IEEE International Conference on Edge Computing (EDGE).* Honolulu, USA. 2017. P. 232–235. DOI: 10.1109/IEEE.EDGE.2017.42.
8. Joshi A., Raturi A., Kumar S., Dumka A., Singh D. P. Improved Security and Privacy in Cloud Data Security and Privacy: Measures and Attacks. *2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP).* Uttarakhand, India. 2022. P. 230–233. DOI: 10.1109/ICFIRTP56122.2022.10063186.
9. Rajasekar P., Kalaiselvi K., Shanmugam R., Tamilselvan S., Pandian A. P. Advancing Cloud Security Frameworks Implementing Distributed Ledger Technology for Robust Data Protection and Decentralized Security Management in Cloud Computing Environments. *2024 Second International Conference on Advances in Information Technology (ICAIT).* Karnataka, India. 2024. P. 1–6. DOI: 10.1109/ICAIT61638.2024.10690718.
10. Kimm H., Ortiz J. Multilevel Security Embedded Information Retrieval and Tracking on Cloud Environments. *2021 IEEE Cloud Summit.* USA. 2021. P. 25–28. DOI: 10.1109/IEEECloudSummit52029.2021.00012.
11. Gnatyuk S., Sydorenko V., Aleksander M. Unified data model for defining state critical information infrastructure in civil aviation. *Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT).* Kyiv. 2018. P. 37–42.
12. Priyadarsini S., Singh A. V., Broumi S. Soft Set Theory: A Conceptual Analysis and Literature Review. *2022 International Conference on Computer Communication and Informatics (ICCCI).* Coimbatore, India. 2022. P. 1–5. DOI: 10.1109/ICCCI54379.2022.9740931.
13. Gnatyuk S. Multilevel Unified Data Model for Critical Aviation Information Systems Cybersecurity. *2019 IEEE 5th International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD).* 2019. P. 242–247.
14. Gnatyuk S., Polishchuk Yu., Sydorenko V., Sotnichenko Yu. Determining the level of importance for critical information infrastructure objects. *PIC S and T 2019: Problems of Infocommunications, Science and Technology.* Kyiv. 2019. P. 829–834.
15. Huang Ch.-Ch., Hsieh Ch.-Ch. Social relevance, then protection: A social-technical approach to CIIP. *2010 International Conference on CISIM.* Krakow, Poland. 2010. P. 239–243. DOI: 10.1109/CISIM.2010.5643658.
16. Jaxymbetova M., Kanayev A., Kossanova I. et al. Improvement of the Mechanical Properties of Reinforcing Bar Steel by Combined Deformation-Heat Treatment. *International Review of Mechanical Engineering (IREME).* 2022. 16(9). P. 460–466. https://doi.org/10.15866/ireme.v16i9.21521
17. Al-Azzeh J., Ayyoub B., Mesleh A. et al. Cloud-Based Information System for Evaluating Caverns in the Process of Blasting Metal Surfaces of Details. *International Review on Modelling and Simulations (IREMOS).* 2025. 18(1). P. 32–42. https://doi.org/10.15866/iremos.v18i1.25596
18. Nur R., Suyuti M., Iswar M., Djalal M. Optimizing the Punch Parameters for V-Bending Stainless Steel Using Response Surface Methodology Approach. *International Review of Mechanical Engineering (IREME).* 2024. 18(1). P. 37–44. https://doi.org/10.15866/ireme.v18i1.23973
19. Yoo S., Kim Y.-W., Choi H. An assessment framework for smart manufacturing. *2018 International Conference on Advanced Communication Technology (ICACT).* Korea. 2018. P. 1–1. DOI: 10.23919/ICACT.2018.8323827.
20. Wei Q. Study on the structure of smart manufacturing system from the perspective of super-network. *2018 Chinese Control and Decision Conference (CCDC).* China. 2018. P. 1482–1487. DOI: 10.1109/CCDC.2018.8407361.
21. Hietala M., Rautio T., Päkkilä J. et al. Exploring the Impact of Surface Quality on the Bending Fatigue Strength of Wire Arc Additive Manufactured Carbon Steel. *ATiGB 2023: Applying New Technology in Green Buildings.* Vietnam. 2023. P. 248–252. DOI: 10.1109/ATiGB59969.20210364399.
22. Hu Z., Gnatyuk S., Akhmetov B. et al. Method for cyber threats detection and identification in modern cloud services. *Advances in Computer Science for Engineering and Education IV. ICCSEEA 2021.* Springer. 2021. P. 326–346. https://doi.org/10.1007/978-3-030-80472-5_28
23. Dawood M., Tu S., Xiao C. et al. Cyberattacks and Security of Cloud Computing: A Complete Guideline. *Symmetry.* 2023. 15. 1981. https://doi.org/10.3390/sym15111981
24. Tu S., Waqas M., Rehman S.U. et al. Security in Fog Computing: A Novel Technique to Tackle an Impersonation Attack. *IEEE Access.* 2018. 6. P. 74993–75001.
25. Fan X., Yao J., Cao N. Research on Cloud Computing Security Problems and Protection Countermeasures. *International Symposium on Cyberspace Safety and Security.* Guangzhou. 2019. P. 542–551.
26. Kuznetsov O., Atzeni G., Arnesano M. et al. Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy. *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications.* 2025. P. 225–257.
27. Kuznetsov O., Smirnov O., Kuznetsova T. et al. Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms. *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications.* 2025. P. 589–622.
28. Kuznetsov O., Smirnov O., Akhmetov B. et al. Deep Learning Frontiers in Copy-Move Forgery Detection: Advances, Challenges, and Future Directions. *Advancements in Cybersecurity Next Generation Systems and Applications.* 2025. P. 202–229.
29. Kuznetsov O., Frontoni E., Kuznetsova Y. et al. Trust-Based Security Architecture for Edge Computing. *CEUR Workshop Proceedings.* 2024. Vol. 3909. P. 227–241.

30. Al-Mudhafar Aqeel A.M., Smirnova T., Buravchenko K., Smirnov O. The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of ML. *Advanced Information Systems.* 2023. 7(2). P. 49–56.
31. Smirnov O., Sydorenko V., Aleksander M. et al. Simulation of the cloud IoT-based monitoring system for critical infrastructures. *CEUR Workshop Proceedings.* 2023. Vol. 3530. P. 256–265.

References

1. Gnatyuk, S., Yudin, O., Sydorenko, V., Smirnova, T., & Polozhentsev, A. (2022). The model for calculating the quantitative criteria for assessing the security level of information and telecommunication systems. *CEUR Workshop Proceedings*, *3156*, 390–399.
2. Cabinet of Ministers of Ukraine. (2020, October 9). *Deiaki pytannia obiektiv krytychnoi infrastruktury* (Resolution No. 1109). https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#n11 [in Ukrainian].
3. Gnatyuk, S., Berdibayev, R., Smirnova, T., Avkurova, Z., & Iavich, M. (2021). Cloud-based cyber incidents response system and software tools. *Communications in Computer and Information Science*, *1486*, 169–184.
4. Ardebili, A. A., Martella, C., Lazari, A., et al. (2024). Smart critical infrastructures security management and governance: Implementation of cyber resilience KPIs for decentralized energy asset. *CEUR Workshop Proceedings*, *3731*. https://iris.unisalento.it/handle/11587/530328.
5. Deloitte. (n.d.). *Bridging measurement divides in AI, cloud, and cyber*. https://www.deloitte.com/us/en/insights/industry/technology/measuring-cyber-ai-and-cloud-kpis.html.
6. Yıldırım, F., Yalman, Y., Bayındır, K. Ç., & Terciyanlı, E. (2025). Comprehensive review of edge computing for power systems: State of the art, architecture, and applications. *Applied Sciences*, *15*(8), 4592. doi.org/10.3390/app15084592
7. Wei, X., et al. (2017). MVR: An architecture for computation offloading in mobile edge computing. In *2017 IEEE International Conference on Edge Computing (EDGE)* (pp. 232–235). IEEE. https://doi.org/10.1109/IEEE.EDGE.2017.42.
8. Joshi, A., Raturi, A., Kumar, S., Dumka, A., & Singh, D. P. (2022). Improved security and privacy in cloud data: Security and privacy measures and attacks. In *2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP)* (pp. 230–233). IEEE. https://doi.org/10.1109/ICFIRTP56122.2022.10063186.
9. Rajasekar, P., Kalaiselvi, K., Shanmugam, R., Tamilselvan, S., & Pandian, A. P. (2024). Advancing cloud security frameworks: Implementing distributed ledger technology for robust data protection and decentralized security management in cloud computing environments. In *2024 Second International Conference on Advances in Information Technology (ICAIT)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICAIT61638.2024.10690718.
10. Kimm, H., & Ortiz, J. (2021). Multilevel security embedded information retrieval and tracking on cloud environments. In *2021 IEEE Cloud Summit* (pp. 25–28). IEEE. https://doi.org/10.1109/IEEECloudSummit52029.2021.00012
11. Gnatyuk, S., Sydorenko, V., & Aleksander, M. (2018). Unified data model for defining state critical information infrastructure in civil aviation. In *Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)* (pp. 37–42). IEEE.
12. Priyadarsini, S., Singh, A. V., & Broumi, S. (2022). Soft set theory: A conceptual analysis and literature review. In *2022 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1–5). IEEE. https://doi.org/10.1109/ICCCI54379.2022.9740931
13. Gnatyuk, S. (2019). Multilevel unified data model for critical aviation information systems cybersecurity. In *2019 IEEE 5th International Conference on Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD)* (pp. 242–247). IEEE.
14. Gnatyuk, S., Polishchuk, Yu., Sydorenko, V., & Sotnichenko, Yu. (2019). Determining the level of importance for critical information infrastructure objects. In *2019 IEEE International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)* (pp. 829–834). IEEE.
15. Huang, C.-Ch., & Hsieh, C.-Ch. (2010). Social relevance, then protection: A social-technical approach to CIIP. In *2010 International Conference on CISIM* (pp. 239–243). IEEE. https://doi.org/10.1109/CISIM.2010.5643658.
16. Jaxymbetova, M., Kanayev, A., Kossanova, I., et al. (2022). Improvement of the mechanical properties of reinforcing bar steel by combined deformation-heat treatment. *International Review of Mechanical Engineering*, *16*(9), 460–466. https://doi.org/10.15866/ireme.v16i9.21521.
17. Al-Azzeh, J., Ayyoub, B., Mesleh, A., et al. (2025). Cloud-based information system for evaluating caverns in the process of blasting metal surfaces of details. *International Review on Modelling and Simulations*, *18*(1), 32–42. https://doi.org/10.15866/iremos.v18i1.25596.
18. Nur, R., Suyuti, M., Iswar, M., & Djalal, M. (2024). Optimizing the punch parameters for V-bending stainless steel using response surface methodology approach. *International Review of Mechanical Engineering*, *18*(1), 37–44. https://doi.org/10.15866/ireme.v18i1.23973.
19. Yoo, S., Kim, Y.-W., & Choi, H. (2018). An assessment framework for smart manufacturing. In *2018 International Conference on Advanced Communication Technology (ICACT)* (p. 1). IEEE. https://doi.org/10.23919/ICACT.2018.8323827.
20. Wei, Q. (2018). Study on the structure of smart manufacturing system from the perspective of super-network. In *2018 Chinese Control and Decision Conference (CCDC)* (pp. 1482–1487). IEEE. https://doi.org/10.1109/CCDC.2018.8407361.
21. Hietala, M., Rautio, T., Päkkilä, J., et al. (2023). Exploring the impact of surface quality on the bending fatigue strength of wire arc additive manufactured carbon steel. In *ATiGB 2023: Applying New Technology in Green Buildings* (pp. 248–252). IEEE. https://doi.org/10.1109/ATiGB59969.20210364399
22. Hu, Z., Gnatyuk, S., Akhmetov, B., et al. (2021). Method for cyber threats detection and identification in modern cloud services. In *Advances in Computer Science for Engineering and Education IV (ICCSEEA 2021)* (pp. 326–346). Springer. https://doi.org/10.1007/978-3-030-80472-5_28.

23. Dawood, M., Tu, S., Xiao, C., et al. (2023). Cyberattacks and security of cloud computing: A complete guideline. *Symmetry*, *15*, 1981. https://doi.org/10.3390/sym15111981.
24. Tu, S., Waqas, M., Rehman, S. U., et al. (2018). Security in fog computing: A novel technique to tackle an impersonation attack. *IEEE Access*, *6*, 74993–75001.
25. Fan, X., Yao, J., & Cao, N. (2019). Research on cloud computing security problems and protection countermeasures. In *International Symposium on Cyberspace Safety and Security* (pp. 542–551).
26. Kuznetsov, O., Atzeni, G., Arnesano, M., et al. (2025). Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy. In *Security and Privacy of Cyber Physical Systems: Emerging Trends, Technologies and Applications* (pp. 225–257).
27. Kuznetsov, O., Smirnov, O., Kuznetsova, T., et al. (2025). Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms. In *Security and Privacy of Cyber Physical Systems: Emerging Trends, Technologies and Applications* (pp. 589–622).
28. Kuznetsov, O., Smirnov, O., Akhmetov, B., et al. (2025). Deep learning frontiers in copy-move forgery detection: Advances, challenges, and future directions. In *Advancements in Cybersecurity: Next Generation Systems and Applications* (pp. 202–229).
29. Kuznetsov, O., Frontoni, E., Kuznetsova, Y., et al. (2024). Trust-based security architecture for edge computing. *CEUR Workshop Proceedings*, *3909*, 227–241.
30. Al-Mudhafar Aqeel, A. M., Smirnova, T., Buravchenko, K., & Smirnov, O. (2023). The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of ML. *Advanced Information Systems*, *7*(2), 49–56.
31. Smirnov, O., Sydorenko, V., Aleksander, M., et al. (2023). Simulation of the cloud IoT-based monitoring system for critical infrastructures. *CEUR Workshop Proceedings*, *3530*, 256–265.

Tetiana Smirnova[1], PhD tech. sci., **Kostiantyn Buravchenko**[1], Assoc. Prof., PhD tech. sci.,
Oleksandr Dobrynchuk[2], jr. researcher, **Serhii Smirnov** [1], Assoc. Prof., PhD tech. sci.,
Nataliia Yakymenko [1], Assoc. Prof., PhD phys.-math. sci., **Oleksii Smirnov**[1], Prof., Dr. tech. sci.,
[1]*Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine*
[2]*State University "Kyiv Aviation Institute", Kyiv, Ukraine*

Cloud-based Technology for Monitoring Key Performance Indicators of Technological Processes in Critical Infrastructure

In this work, a cloud technology was developed for monitoring key performance indicators of critical infrastructure technological processes in real time in order to detect deviations in technological processes, as well as to prevent attacks (failures) by analyzing anomalous equipment behavior, changes in load modes, resource consumption, etc. The tuple model of key performance indicators was further developed, which allows systematizing monitoring parameters in information and communication systems of critical infrastructure objects, formalizing automatic data processing, supporting integration with analytical cloud platforms, as well as identifying deviations (anomalies), cyber incidents, degradation, excessive load or sabotage and, as a result, preparing aggregated key performance indicators for daily monitoring by operators and IT services. A model of the technological process of electric arc processing in UAV engineering is proposed, which in the conditions of the current stage of the Russian-Ukrainian war is part of the critical infrastructure in the economy and defense-industrial production sector. This is due to the fact that UAVs now play a crucial role on the battlefield. A scheme for monitoring key performance indicators for the electric arc processing technological process has been developed. For this, the use of cloud technologies is proposed, a general scheme of the electric arc processing technological process in UAV engineering is given, with their use. An example of a model infrastructure based on the Azure cloud platform has been implemented. The data model is presented in JSON format (which is effective for API, MQTT broker or Kafka). Verification of the model on empirical data confirmed its compliance with the requirements, resistance to changing conditions and great significance for monitoring technological processes in critical infrastructure. In the context of digitalization and countering cyber risks, the model is the basis for creating a digital twin of the production system. Thus, reliability, predictability and security are ensured. The paper proposes integration with artificial intelligence/machine learning (AI/ML) algorithms, such as LSTM, which allows for real-time advanced analytics, adaptive process control, and automated decision-making. In the future, the LSTM algorithm can be used to build a model for predicting the parameters of key performance indicators in an electric arc processing system, and other AI/ML and data mining algorithms that can process large volumes of time series and take into account complex nonlinear dependencies between technological parameters can also be used.

cloud technology, technological processes, critical infrastructure, information and communication system, electric arc processing, UAV, cyber risks, cybersecurity, IoT, artificial intelligence, machine learning

Одержано (Received) 11.09.2025 *Прорецензовано (Reviewed) 17.10.2025*
Прийнято до друку (Approved) 28.10.2025